AGÊNCIA NACIONAL DO CINEMA

PORTARIA ANCINE N.º 489-E, DE 14 DE AGOSTO DE 2018

Institui diretrizes para os processos de Gestão de Riscos, Gestão de Continuidade e Gestão de Mudanças, nos aspectos relativos à Segurança da Informação e Comunicações na Agência Nacional do Cinema - ANCINE.

O **DIRETOR-PRESIDENTE DA AGÊNCIA NACIONAL DO CINEMA – ANCINE**, no uso das atribuições que lhe confere o inciso IV do art. 13 do Anexo I do Decreto nº. 8.283, de 3 de julho de 2014, bem como o disposto no inciso III do art. 17 do Regimento Interno da ANCINE, Resolução de Diretoria Colegiada nº. 59, de 2 de abril de 2014, e **CONSIDERANDO:**

o Decreto nº 3.505, de 13 de Junho de 2000, que institui a Política de Segurança da Informação nos Órgãos da Administração Pública Federal;

a Resolução de Diretoria Colegiada nº. 63, de 23 de setembro de 2014, a qual institui a Política de Segurança da Informação e Comunicações da Agência Nacional do Cinema – ANCINE, e dá outras providências;

a Resolução de Diretoria Colegiada Resolução de Diretoria Colegiada nº. 78, de 06 de setembro de 2017, a qual dispõe sobre a política de gestão de riscos e sobre o Comitê de Governança, Riscos e Controles da Agência Nacional do Cinema – ANCINE;

a Instrução Normativa nº 1, do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, a qual disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

a Norma Complementar nº 04/IN01/DSIC/GSIPR, do Departamento de Segurança da Informação e Comunicações, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos ou entidades da Administração Pública Federal - APF, direta e indireta;

a Norma Complementar nº 06/IN01/DSIC/GSIPR, que estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

a Norma Complementar nº 07/IN01/DSIC/GSIPR, que estabelece Diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicações;

a Norma Complementar nº 13/IN01/DSIC/GSIPR, que estabelece Diretrizes para Gestão de Mudanças nos aspectos relativos à segurança da informação e comunicações nos órgãos e entidades da administração pública federal;

a Norma ABNT NBR ISO/IEC 27002:2005, que trata de Código de Pratica para a gestão da Segurança da Informação;

a Norma ABNT NBR ISO/IEC 27005:2011, que trata de Gestão de Riscos de Segurança da Informação;

a Norma Técnica ABNT NBR ISO/IEC 22301:2013, que normatiza o sistema de gestão de continuidade de negócios e especifica os requisitos para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente um sistema de gestão documentado para se proteger, reduzir a possibilidade de ocorrência, preparar-se, responder e recuperar-se de incidentes de interrupção quando estes ocorrerem.

RESOLVE:

Art. 1º Aprovar, por meio desta Portaria e de seu anexo, diretrizes para a Gestão de Riscos, para a Gestão de Continuidade e para a Gestão de Mudanças, nos aspectos relativos à Segurança da Informação e Comunicações (SIC), em complemento às disposições gerais de Gestão de Riscos da Agência Nacional do Cinema – ANCINE**.**

Parágrafo único. As atividades relativas aos processos de Gestão de Riscos, de Continuidade e de Mudanças serão realizadas, sempre que possível, de forma integrada.

Art. 2º Para dar suporte às atividades de Gestão de Riscos, de Continuidade e de Mudanças relativos à SIC, os ativos de informação da ANCINE serão mapeados pela Gerência de Tecnologia da Informação (GTI).

Parágrafo único. Durante a realização do mapeamento, os ativos de informação serão classificados em níveis de criticidade, segundo o Anexo I desta Portaria, considerando o tipo de ativo de informação e o provável impacto no caso de quebra de segurança.

CAPÍTULO I
DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para efeitos desta norma, ficam estabelecidos os seguintes termos e definições, em complemento àqueles definidos na Política de Segurança da Informação e Comunicações da ANCINE e na Política de Gestão de Riscos da ANCINE:

I – Análise de Impacto nos Negócios (AIN): visa estimar os impactos resultantes da interrupção de serviços e de cenários de desastres que possam afetar o desempenho dos órgãos ou entidades da APF, bem como as técnicas para quantificar e qualificar esses impactos. Define também a criticidade dos processos de negócio, suas prioridades de recuperação, interdependências e os requisitos de segurança da informação e comunicações para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos;

II – Agente Responsável pela Classificação e Identificação de Ativos de Informação: Servidor Público ocupante de cargo efetivo, incumbido de chefiar e gerenciar o processo de Classificação e Identificação de Ativos de Informação;

III – Continuidade de Negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

IV – Gestão de Continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado;

V – Gestão de Mudanças nos aspectos relativos à SIC: é o processo de gerenciamento de mudanças, de modo que ela transcorra com mínimos impactos no âmbito do órgão ou entidade da Administração Pública Federal (APF), visando viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação;

VI – Gestão de Riscos de Segurança da Informação e Comunicações: conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

VII – Classificação e Identificação de Ativos de Informação: é um processo interativo e evolutivo, composto por 3 (três) etapas: (a) identificação e classificação de ativos de informação, (b) identificação de potenciais ameaças e vulnerabilidades e (c) avaliação de riscos;

VIII – Plano de Continuidade de Negócios: documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da Administração Pública Federal (APF) mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes;

IX – Plano de Gerenciamento de Incidentes: plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente que, basicamente, cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;

X – Plano de Recuperação de Negócios: documentação dos procedimentos e informações necessárias para que o órgão ou entidade da APF operacionalize o retorno das atividades críticas a normalidade;

XI – Programa de Gestão da Continuidade de Negócios: processo contínuo de gestão e governança suportado pela alta direção e que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por intermédio análises críticas, testes, treinamentos e manutenção;

XII – Proprietário do ativo de informação: refere-se a parte interessada do órgão ou entidade da APF, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação, assumindo, no mínimo, as seguintes atividades: a) descrever o ativo de informação; b) definir as exigências de segurança da informação e comunicações do ativo de informação; c) comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários; d) buscar assegurar-se de que as exigências de segurança da informação e comunicações estejam cumpridas por meio de monitoramento; e, e) indicar os riscos que podem afetar os ativos de informação;

XIII – Riscos de Segurança da Informação e Comunicações: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização; e

XIV – Valor do Ativo de Informação: valor, tangível e intangível, que reflete tanto a importância do ativo de informação para o alcance dos objetivos estratégicos de um órgão ou entidade da APF, quanto o quão cada ativo de informação é imprescindível aos interesses da sociedade e do Estado.

CAPÍTULO II

DA GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Art. 4º O processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC, além de estar em consonância com o Planejamento Estratégico, a Política de Segurança da Informação e Comunicações, e a Política de Gestão de Riscos da ANCINE, deverá:

I – garantir que sistemas estruturantes tenham padrões mínimos de Segurança da informação e de Comunicações – SIC, conforme definido na Norma Complementar nº 19/IN01/DSIC/GSPR;

II – promover a alta confiabilidade para tratar informação em termos de confidencialidade, integridade e disponibilidade;

III – preservar o valor do investimento em tecnologia, informação, processos e conhecimento;

IV – proteger as informações utilizadas para decisões importantes;

V – garantir a satisfação de requisitos legais e de regulação;

VI – reduzir o custo de incidentes de segurança; e

VII – garantir a continuidade do trabalho.

Art. 5º O processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC será contínuo e aplicado na implementação e na operação da Gestão de Segurança da Informação e Comunicações.

§1º. O processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC será aprimorado continuamente, com base em metodologia definida na Norma Complementar nº 02/IN01/DSIC/GSIPR.

§2º. A metodologia e os procedimentos adotados na GRSIC devem, sempre que possível, estar em consonância com aqueles adotados no âmbito da Política e do Plano de Gestão de Riscos da ANCINE.

Art. 6º Com o objetivo de manter os riscos em níveis aceitáveis, serão adotados os procedimentos definidos no item 6, da Norma Complementar nº 04/IN01/DSIC/GSI/PR.

CAPÍTULO III
DA GESTÃO DE CONTINUIDADE DE NEGÓCIOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Art. 7º A gestão de continuidade de negócios de segurança da informação e comunicações tem como objetivo:

I – reduzir o risco e minimizar o impacto de interrupções dos serviços e sistemas de TIC que suportam as atividades críticas da ANCINE;

II – manter os sistemas e serviços críticos de TIC em um nível minimamente operável e aceitável durante a ocorrência de um desastre, de forma a não interromper a prestação de serviços pela ANCINE;

III – definir procedimentos para que as atividades críticas operem em nível de contingência quando da ocorrência de um desastre ou interrupção não programada, até que a situação retorne à normalidade; e

IV – proceder à recuperação de ativos de informação a um nível aceitável, combinando ações de prevenção, resposta e recuperação.

Art. 8º A Gerência de Tecnologia da Informação (GTI) instituirá o Programa de Gestão da Continuidade de Negócios de forma a assegurar a disponibilidade dos ativos de informação e a recuperação das atividades críticas.

Art. 9º O Programa de Gestão da Continuidade de Negócios será composto por, no mínimo:

I – Plano de Continuidade de Negócios – PCN;

II – Plano de Gerenciamento de Incidentes – PGI; e

III – Plano de Recuperação de Negócios – PRN.

Parágrafo único. Os referidos planos serão elaborados em conformidade com os requisitos mínimos estabelecidos pelo item 5, da Norma Complementar nº 06/IN01/DSIC/GSIPR.

Art. 10. A gestão de continuidade deve observar o resultado das análises de riscos do processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC e da análise de impacto de negócio realizadas, de forma a nortear as estratégias de continuidade.

Art. 11. A análise de impacto de negócio incluirá:

I – identificação das atividades que suportam o fornecimento de produtos e serviços;

II – avaliação dos impactos de não realização das atividades ao longo do tempo;

III – fixação dos prazos de forma priorizada para a retomada das atividades, em um nível mínimo de execução tolerável, levando em consideração o tempo em que o impacto da interrupção torne-se inaceitável; e

IV – identificação de dependências e recursos que suportam as atividades, incluindo fornecedores, terceiros e demais partes interessadas relevantes.

CAPÍTULO IV
DA GESTÃO DE MUDANÇAS NOS ASPECTOS RELATIVOS À SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Art. 12. O processo de Gestão de Mudança tem o propósito de controlar o ciclo de vida de todas as mudanças, permitindo mudanças benéficas ao negócio com o mínimo de interrupções para os serviços de TI.

Parágrafo único. O gerenciamento de mudanças será composto pelas fases de Descrição, Avaliação, Aprovação, Implementação e Verificação, de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, e será realizado de acordo com procedimentos a serem estabelecidos pela Gerência de Tecnologia da Informação.

Art. 13. O processo de Gestão de Mudança contemplará as diretrizes estabelecidas pelo Planejamento Estratégico da ANCINE e tem por objetivos:

I – responder aos requerimentos de mudanças necessárias nos serviços, maximizando valor e reduzindo incidentes, rupturas e retrabalhos;

II – responder às solicitações de negócio e de TI para mudanças que irão alinhar os serviços com as necessidades do negócio; e

III – assegurar que as mudanças sejam registradas, avaliadas, autorizadas, priorizadas, planejadas, testadas, implementadas.

CAPÍTULO V
DA IDENTIFICAÇÃO E CLASSIFICAÇÃO DE ATIVOS DE INFORMAÇÃO

Art. 14 Constituem etapas da Identificação e Classificação de Ativos de Informação:

I – coleta de informações gerais dos ativos de informação;

II – detalhamento dos ativos de informação;

III – identificação dos responsáveis, proprietários e custodiantes, de cada ativo de informação;

IV – caracterização dos contêineres dos ativos de informação;

V – definição dos requisitos de segurança da informação e comunicações; e

VI – estabelecimento do valor do ativo de informação.

Parágrafo único. A Gerência de Tecnologia da Informação (GTI), quando solicitada pelo Agente Responsável, prestará auxílio para a execução do processo de Identificação e Classificação de Ativos de Informação.

CAPÍTULO VI
DAS RESPONSABILIDADES

Art. 15. Compete ao Comitê de Governança, Riscos e Controle aprovar as diretrizes gerais e estratégicas, bem como os respectivos planos para os processos de Monitoramento de Ativos de Informação, de Gestão de Riscos, de Gestão de Continuidade, e Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações.

Art. 16. Cabe ao Comitê de Segurança da Informação e Comunicações, em conformidade com a Gestão Estratégica da ANCINE, com a Política de Segurança da Informação e Comunicações e com a Política de Gestão de Riscos da ANCINE:

I – propor as diretrizes gerais e monitorar o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC;

II – propor as diretrizes estratégicas do Programa de Gestão da Continuidade de Negócios;

III – propor estratégias, planos, processos e decidir sobre ações de melhorias e correções em relação à Continuidade de Negócios e à Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC;

IV – avaliar e aprovar a Análise de Impacto nos Negócios; e

V – avaliar e propor revisões periódicas no processo de gestão de mudanças.

Parágrafo único. O Núcleo de Gestão de Riscos realizará o acompanhamento da execução dos procedimentos relativos à Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC.

Art. 17. Cabe ao Gestor de Segurança da Informação e Comunicações, no âmbito de suas atribuições:

I – coordenar a Gestão de Riscos de Segurança da Informação na ANCINE;

II – coordenar a realização periódica da Análise de Impacto nos Negócios;

III – coordenar a Classificação e Identificação de Ativos de Informação e analisar os resultados obtidos no controle dos níveis de segurança da informação e comunicações de cada ativo de informação;

IV – supervisionar a elaboração, a implementação, os testes e a atualização dos Planos previstos no Programa de Gestão da Continuidade de Negócios;

V – planejar, implementar e monitorar os processos de Gestão de Mudanças sobre aspectos relacionados à Segurança da Informação e Comunicações na ANCINE, assumindo as responsabilidades previstas para o Gestor de Mudanças;

VI – recomendar a implementação ou não das mudanças propostas, indicando, sempre que possível, soluções que mitiguem riscos à SIC; e

VII – comunicar, sempre que necessário, o teor das deliberações, das atividades e das normas relativas à Continuidade de Negócios, à Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC, e ao processo de gestão de mudanças.

Parágrafo único. O Gestor de Segurança da Informação e Comunicações poderá indicar responsáveis pelo gerenciamento de atividades mencionadas.

Art. 18. Cabe ao Agente Responsável pela Classificação e Identificação de Ativos de Informação:

I – identificar e classificar os ativos de informação;

II – monitorar os níveis de segurança dos ativos de informação junto aos proprietários e custodiantes dos ativos de informação; e

III – elaborar a sistemática de relatórios para os Gestores de Segurança da Informação e Comunicações.

CAPÍTULO VII
DAS DISPOSIÇÕES FINAIS

Art. 19. Os casos não previstos nesta norma serão submetidos à apreciação do Comitê de Segurança da Informação e Comunicações.

Art. 20. Esta norma entra em vigor na data de sua publicação.

ANEXO I

MODELO DE CLASSIFICAÇÃO DE ATIVOS DE INFORMAÇÃO

Grau de Criticidade	Ativos de Informação	Impacto	Cor
Nível 1 Alto	Datacenter (CPD), servidores, recursos criptológicos, cópias de segurança, equipamentos de conectividade ou de armazenamento de informações ou de computação móvel das autoridades de primeiro escalão.	Interrompe a missão do órgão ou provoca grave dano à imagem institucional, à segurança do estado ou sociedade.	Vermelha
Nível 2 Médio	Computadores com dados e informações únicas, de grande relevância, equipamentos de conectividade ou de armazenamento de informações ou de computação móvel das autoridades de segundo escalão.	Degrada o serviço do órgão ou provoca dano à imagem institucional, à segurança do estado ou sociedade.	Amarela
Nível 3 Baixo	Os demais ativos de informação	Compromete planos ou provoca danos aos ativos de informação.	Sem cor